法定通訊監察技術說明

籠罩在一團謎霧及爭論之下，通訊監察向來是一難以通盤瞭解及確切執行的計畫方案。不像其他軟體，與此相關的技術文件及網路社群討論相當罕見，若沒有適當的管道或相當的費用，幾乎拿不到相關的訊息。

即便如此，市場上仍然有一些通訊監察解決方案供應商，寡占了整個利基市場。這些寡占解決方案供應商盡一切力量控制市場，並凸顯其所屬解決方案的複雜性。有鑑於此，定興科技於十年前以台灣所擁有強大的科技研發資源投入此一領域，開發出一系列符合 ETSI 和 CALEA 規範的通訊監察系統，行銷全球五十餘國。

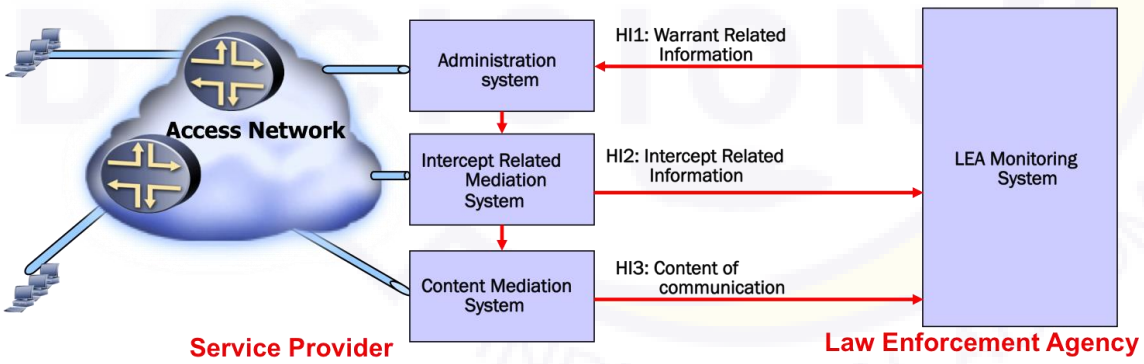
此外電信營運商也必須依相關電信法規的要求，為執法單位提供通訊監察的網路資料傳輸界面。其下將會就相關細節做一介紹。並以目前市場上符合 ETSI 規範通訊監察解決方案的為例。

通訊監察是什麼 ？

通訊監察任務的主要項目是由執法單位從電信營運商的網路系統中靜默地取得受監控目標的網路通訊，截取到相關的通訊封包流量或語音以作為資料分析或呈堂證據。這些資料通常包括語音訊號、網路數據封包、或者在某些情況下有通訊內容。假如資料無法即時取得，那麼就必須從電信營運商的備分資料裝置中取得。

此外我國所有通訊監察建置還必須依《中華民國通訊監察及保護法》相關規定辦理。

綜觀通訊監察



通常電信營運商將提供三個規範資料交換界面(HI)與執法單位後台的通訊監察管理系統(LEMF)連結。這也是資料截取及分析的規範需求。

ETSI 規範界面項目:

- HI1
- HI2
- HI3
- HIA (圖片中未顯示)
- HIB (圖片中未顯示)

HI1

此交換界面主要是提供一個通道讓後台通訊監察管理系統所發出執行傳票的命令,可由此轉給前端通訊監察中介器(Mediation device)。此外也可經由此界面,傳回網路系統的狀態資訊,如上線時間、目標狀態、效能狀況、可用狀態等等。其中有:

- 目標資料(被監控者)
- 監控期限
- 對應監控資料(針對 HI2 及 HI3 對應相關資料)

HI2

此交換界面主要是提供一個通道讓目標監察通訊狀態資料(IRI) 傳回到後台通訊監察管理系統。真正的通訊監察內容並不由此傳送,也不經由此被側綠。監察通訊狀態資料所包含的訊息有被監控目標在期間所有的動作。簡單的說,譬如一件電子郵件由 A 送至 B,其內容並不經由此傳送,但發送者及接收者和其他表頭資料會成為監察通訊狀態資料的一部分。 由 ETSI 所定義的監察通訊狀態資料是採用 ASN.1 格式,並以 BER 格式碼來加密傳送。

HI3

這一個交換界面 HI3 是用來作通訊內容資料(CC)的傳送,前面曾提到通訊狀態資料(IRI)這一 部分。於此不同處,通訊內容資料是構成 HI3 交換界面的核心部分。當資料傳送到後台通訊監察管理系統時,有數種定義資料格式可供選擇採用。ETSI 並未強迫使用哪一種格式,不同的後台可以採行其中一種來使用。就目前市場上的通行傳回到後台通訊監察管理系統,以下是較通用常見的格式:

- BER encoded ASN.1 – 每一檔案僅單一封包
- BER encoded ASN.1 – 每一檔案有數個封包
- PCAP
- 以 q931 次頻道關聯資料經語音 E1 線路傳送

HIA

最後兩個是用來處理儲存的資料。第一個儲存資料交換界面 HIA 是用來作資料查詢接收使用，這一類資料查詢主要有兩個項目：監控期限及監控目標。

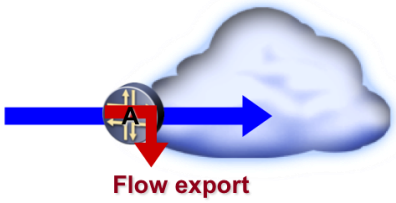
HIB

最後一個儲存資料交換界面 HIB 是用來作產生回應由 HIA 來的資料查詢的目標監察通訊狀態資料。

通訊監察建置

主動式封包攔截

Active Flow Monitoring

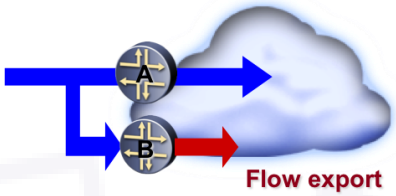


Router (A) forwards packets and exports flow records

Router (A) performs routing, forwarding, and exporting of flows

Monitors ingress or egress flows

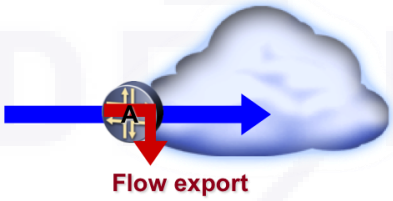
Passive Flow Monitoring



- Router (A) forwards packets
- Router (B) performs passive monitoring and exports flow records
  - Router (B) does not participate in the control or data plane of network
- Monitors multiple OC3, OC12, OC48s

被動式封包攔截

Active Flow Monitoring

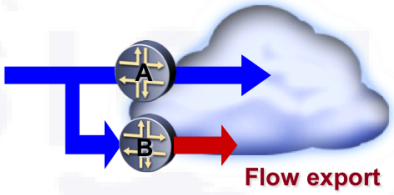


Router (A) forwards packets and exports flow records

Router (A) performs routing, forwarding, and exporting of flows

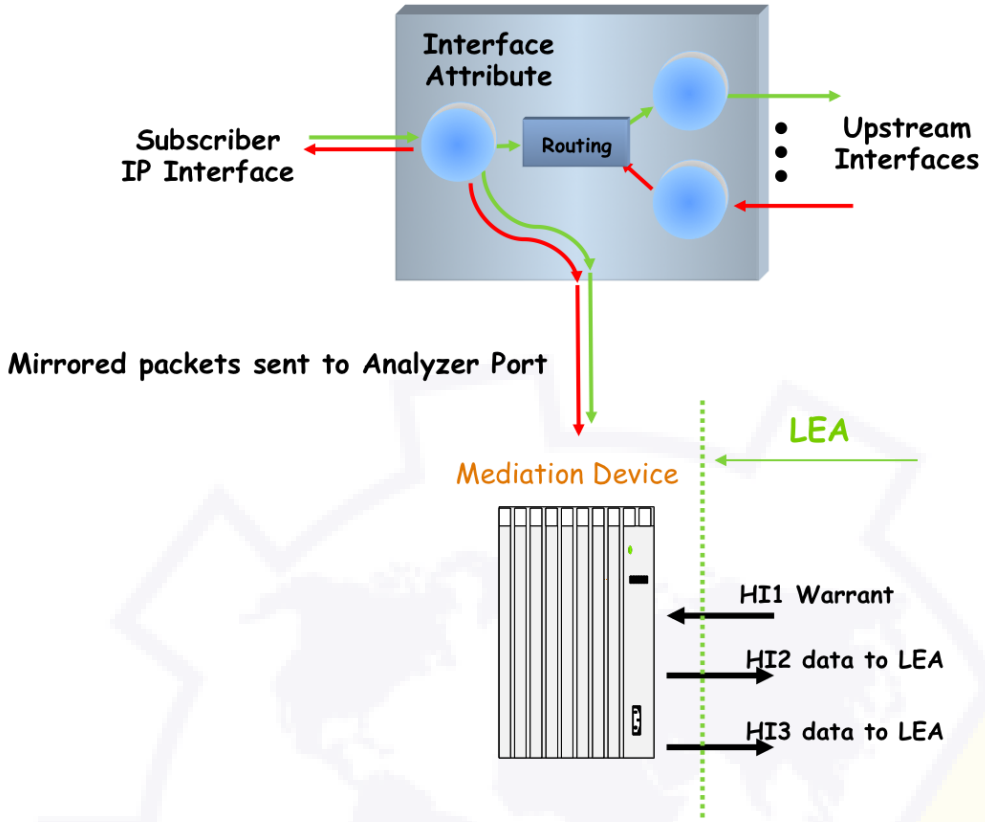
Monitors ingress or egress flows

Passive Flow Monitoring

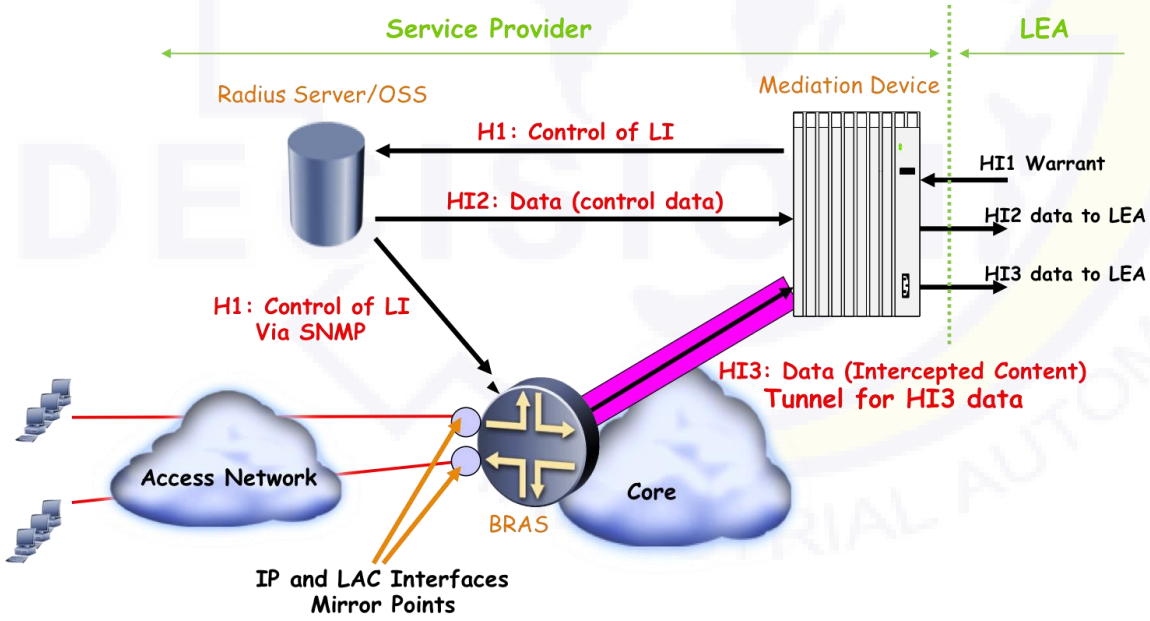


- Router (A) forwards packets
- Router (B) performs passive monitoring and exports flow records
  - Router (B) does not participate in the control or data plane of network
- Monitors multiple OC3, OC12, OC48s

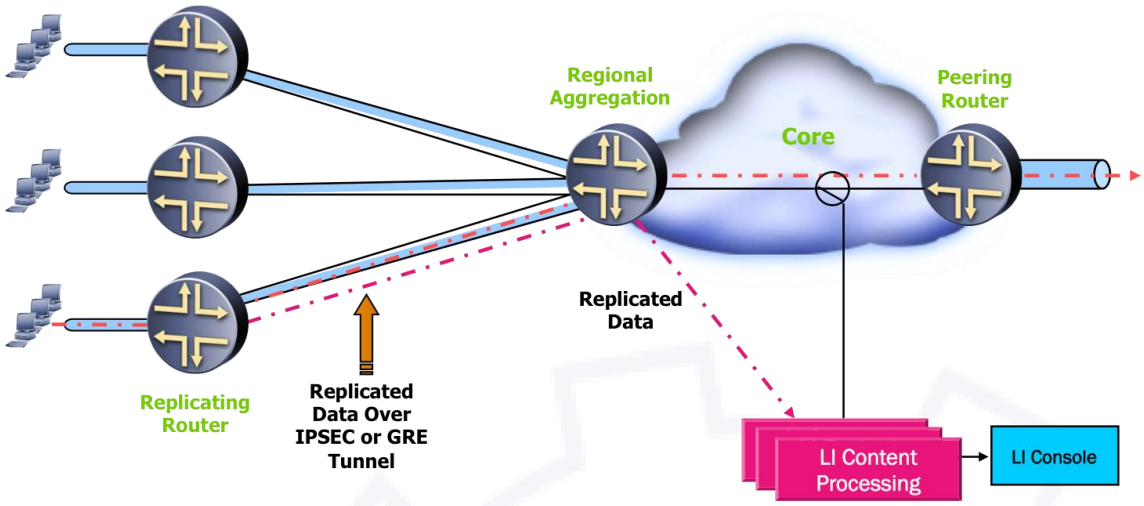
被動式監控 –如何運作?



主動式監控 – 如何運作?



標準建置



適用定義規範

- ETSI TS 102-232-1
- ETSI TS 102-232-2
- ETSI TS 102-232-3
- ETSI TS 102-232-4
- ETSI TS 102-232-5
- ETSI TS 102-232-6
- ETSI TS 102-656
- ETSI TS 102-657
- ETSI TS 101-671

上述規範是定義什麼?

若你沒聽說過 ETSI TS 102-232，大概你還沒有接觸過建置通訊監察系統。這一系列的規範是提供了各項通訊服務的監控方式及資料範圍，如下列範圍:

- EMAIL 服務
  - POP3
  - IMAP
  - SMTP

- WEBMAIL 服務
- Layer 3 網路層截取
  - RADIUS Username targeting
  - IP Targeting
- Layer 2 媒介層截取
  - DHCP targeting (MAC Address or Option 82)
  - MAC Address Targeting
- HTTP
- MSN
- IRC
- SIP

此外針對無線網路通訊，如 3G 和 4G 網路，也有相關的一些通訊監察規範以符合 3GPP 規範下的網路架構特殊需求，如下列:

- ETSI TS 133 106
- ETSI TS 133 107
- ETSI TS 133 108

資料儲存

- 是選擇將所有 HI2 資料存入到資料庫，以保有整個網路資料而非僅單一目標
- 依國家法 律在規定期限內保存資料，通常兩年
- 是選擇將所有 HI3 資料(CC)存入到大容量儲存裝置中
- 定期將已過法定期限的歸檔資料，依程序清理刪除

以上所述及各項前後台通訊監察裝置，定興皆提供相關軟硬體系統。如有針對貴單位(法定通訊監察機關或電信營運商)有特殊通訊監察需求，請致電 (02) 2766 5753 或電子信箱: decision@decision.com.tw，本公司專業資深技術服務人員將揭誠為您提供詳盡解決方案。

(本文部分內容及圖片採自 Juniper 公司文件)